PSR for Android

Handbuch

2.30 — Letzte Änderung: October 30, 2014

MATESO GmbH

Inhaltsverzeichnis

Vorwort **1**
Sicherheit **2**
Installation **3**
Bedienung **4**
Datenbanken **5**
Erstellen von Datenbanken 6
Öffnen von Datenbanken 7
Datenbanken löschen 8
Datensätze **9**
Erstellen von Datensätzen 10
Bearbeiten von Datensätzen 11
Passwort erzeugen 12
Ordner **13**
Erstellen von Ordnern 15
Bearbeiten und Löschen von Ordnern 16
Formulare **17**
Erstellen von Formularen 18
Bearbeiten von Formularen 19
Internet Browser **20**
Automatische Passworteintragung 21
Favoriten und Lesezeichen **22**
Allgemeine Favoriten 23
GeoFav 24
Lesezeichen 25
Synchronisierung **26**
WLAN Synchronisation 27
Google Drive Synchronisation / Backup 36
Dropbox Synchronisation / Datensicherung 39
Airpass **42**
Einstellungen **43**
Einstellungen am Password Safe Client 45
Support **47**
Lizenzbestimmungen **48**

Vorwort

Password Safe App für Android

Herzlich Willkommen bei der Android App von Password Safe and Repository, der führenden Komplettlösung im Bereich Passwort- und Identitätsmanagement.

Seit mittlerweile über 12 Jahren ist Password Safe zu einer leistungsstarken und funktionsreichen Software gereift. Es erklärt sich von selbst, dass wir unseren Kunden das leistungsfähige Tool zur Passwortverwaltung nun auch in Form einer mobilen App zur Verfügung stellen. Ganz und gar nicht selbstverständlich ist es jedoch, dass diese App wie im vorliegenden Fall kostenlos zur Verfügung gestellt wird.

Egal ob im Beruf oder Privat: Immer mehr Anwendungen benötigen persönliche Passwörter um eine verlässliche Authentifizierung der Person zu gewährleisten. Aufgrund des immer größer werdenden Stellungswertes von mobilen Endgeräten ist es unabdingbar, dass die immense Anzahl von Passwörtern auch mobil zur Verfügung steht. Abschließend beinhaltet ein zukunftsorientiertes Konzept selbstverständlich noch die Möglichkeit der Synchronisation mit den Passwörtern auf Ihrem PC oder Notebook.

Genau diesen Ansatz verfolgen wir mit dieser Anwendung. Mit Bravour meistert Password Safe den Spagat zwischen dem professionellen Schutz Ihrer Daten und intuitiver Bedienelemente. Unser Passwort Generator gewährleistet dabei stets, dass ausschließlich sichere Passwörter eingesetzt werden und erstellt für Sie sichere und komplexe Passwörter auf Knopfdruck.

Falls Sie Fragen oder Anmerkungen zur folgenden Hilfe haben wenden Sie sich bitte direkt an support@passwordsafe.de.

Ihr Password Safe Team

Sicherheit

Ihre Sicherheit ist unser Bestreben

- Verschlüsselung mit 256-Bit AES Algorithmus
- Durch Salted Hashes sicher vor Rainbowtable-Angriffen
- Generiert sichere und komplexe Passwörter auf Knopfdruck
- Verwaltung mehrerer Datenbanken
- Verschlüsselte Datensicherung und Synchronisierung mit Dropbox und Google Drive
- Zerstörungs-Modus bei zu vielen Anmeldeversuchen (optional)
- Ablaufdatum für die Datenbank (optional)

Tipps für sichere Passwörter

Folgende Richtlinien geben Ihnen einige Hinweise, wie Sie sich selbst ein sicheres und dabei trotzdem leicht zu merkendes Passwort erstellen können (z.B.: für das Passwort einer Password Safe Datenbank)

- Ein sicheres Passwort sollte mindestens 10 Zeichen lang sein. Richtig sicher ist es aber erst ab 15 Zeichen
- Ein sicheres Passwort besteht aus Zahlen, Satz- und Sonderzeichen. Außerdem enthält es Groß- und Kleinbuchstaben
- Kann man Ihr Passwort im Duden oder einem anderen Wörterbuch nachschlagen, ist es nicht sicher genug. Passwort-Knacker-Programme (Brute-Force-Attacke) arbeiten mit solchen Wörterbüchern und probieren deren Einträge systematisch aus.
- Der eigene Name, Namen von Angehörigen, der Name des Haustiers, Telefonnummern, Autonummern, Geburtstage und andere Daten, die man mit einer Recherche über Sie herausbekommen kann, sind als Passwörter untauglich. Das gleiche gilt für Zahlen wie Pi.
- Vermeiden Sie Tastaturmuster wie asdf und jklö.
- Bilden Sie Passwörter, indem Sie die Anfangsbuchstaben aus einem leicht zu merken Satz verwenden. “Ab jetzt will ich für meinen PC nur noch sichere Passwörter verwenden” ergibt Ajw1fmPnnsPv (zusätzlich wurde hier z.B. i durch 1 ersetzt).
- Eine weitere Methode ist die Vermischung von Zahlen und Wörtern: K2e9n1n0w2o0r0t1 aus Kennwort und 29.10.
- Das Datum sollte dabei kein bekannter Geburtstag sein.

Installation

Die Password Safe App können Sie (wie gewohnt) über den Google Play Store herunter laden. Sie wird dann automatisch auf Ihrem Smartphone installiert. Sie ist mit allen Smartphones und Tablets mit Android ab Version 2.2 oder neuer kompatibel.

Bedienung

In diesem Kapitel wird die grundsätzliche Bedienung der Password Safe App beschrieben. Weiterhin lernen Sie hier die einzelnen Bedienelemente kennen.

Nach dem Anmelden an einer Datenbank, sehen Sie oben die Menüleiste. Hier können Sie zwischen verschiedenen Ansichten umschalten:

Alle Passwörter werden alphabetisch geordnet dargestellt.
Hier sehen Sie Ihre Favoriten und geoFavs.
Rufen Sie hier (alphabetisch geordnet) alle Datensätze mit einer URL ab.
Hier sehen Sie die Datensätze in einer Ordnerstruktur (ähnlich wie z.B. auch am Password Safe Client).

Datenbanken

Was sind Datenbanken?

Um Passwörter zu speichern, wird eine Datenbank benötigt, in welcher die Daten abgelegt werden können. Die Datenbank wird lokal auf dem Smartphone bzw. Tablet abgelegt. Die Sicherheit der Datenbank hängt von der Passwortstärke ab. Ein komplexes Passwort ist sicherer als ein vierstelliger Code.

Erstellen von Datenbanken

Die Datenbank kann im Login Screen durch Klick auf das **+** Symbol erstellt werden.

Es folgt ein Dialog, in welchem Sie der Datenbank einen Namen geben können. Darunter finden Sie die Möglichkeit die Verschlüsselungsmethode auszuwählen.

PIN
Ist diese Option aktiviert, wird die Datenbank mit einer vierstelligen PIN verschlüsselt. Hierdurch wird der Zugriff auf die Datenbank vereinfacht.

Passwort
Ist die Option Passwort aktiviert, wird die Datenbank mit einem komplexen Passwort verschlüsselt. Hier können Sie die Länge des Passworts und die zu verwenden Zeichen frei wählen. Es sind also nicht nur Ziffern, sondern auch Klein- und Großbuchstaben, sowie Sonderzeichen möglich. Diese Option bietet zwar weniger Komfort als ein einfaches Passwort, dafür ist jedoch ein höherer Schutz gegeben.

Muster
Über die Option Muster können Sie die Datenbank auch mit dem von Android gewohnten Pattern verschlüsseln.

Nachdem Sie den Namen der Datenbank festgelegt und sich für ein einfaches oder komplexes Passwort entschieden haben, klicken Sie einfach auf Speichern um die Datenbank zu erstellen. Es folgt ein Dialog, in welchem Sie das Passwort der Datenbank vergeben. Nach dem dies geschehen ist, müssen Sie das Passwort zur Sicherheit noch einmal wiederholen.

Öffnen von Datenbanken

Datenbanken löschen

Sollte eine Datenbank nicht mehr benötigt werden, so kann diese gelöscht werden. Hierfür klicken Sie im Login Screen lange auf den entsprechenden Eintrag. Es erscheint dann die Schaltfläche Datenbank Löschen. Nach einem klick darauf müssen Sie das Passwort der Datenbank eingeben. Anschließend wird diese gelöscht.

Datensätze

Was sind Datensätze?

In Datensätzen werden Ihre Anmeldedaten wie Benutzername, Passwörter oder Internetadressen gespeichert. Jedem Datensatz wird ein Formular zugeordnet, welches festlegt, welche Felder im Datensatz angelegt werden können.

Erstellen von Datensätzen

Um einen neuen Datensatz anzulegen, wechseln Sie zunächst in den Ordner, in welchem das Passwort hinterlegt werden soll. Anschließend klicken Sie auf das + Symbol und wählen im nächsten Dialog **Datensatz erstellen**.

Anschließend wird Ihnen der neue Datensatz mit vorbelegten Feldern angezeigt. Sie können direkt die entsprechenden Felder anklicken, um diese zu ändern. Beachten Sie, dass die je nach verwendetem Formular unterschiedliche Felder zur Verfügung stehen. Nachdem Sie alle Felder entsprechend Ihren Wünschen angepasst haben, klicken Sie links oben auf **Speichern**. Sollten Sie eines der Felder nicht benötigen, so können Sie auf das X hinter dem jeweiligen Feld klicken. Es erscheint ein Dialog, in welchem Sie das Löschen noch kurz bestätigen müssen.

Benötigen Sie für diesen einen Datensatz ein weiteres Feld, so klicken Sie einfach auf **Feld hinzufügen** und im nächsten Dialog auf **Feld erstellen**. Im folgenden Screen können Sie das Feld an Ihre Anforderungen anpassen.

Bearbeiten von Datensätzen

Ändern von Datensätzen

Um einen Datensatz zu ändern, klicken Sie einfach einmal darauf und anschließend auf das **Stiftsymbol**. Nun können Sie direkt in das zu bearbeitende Feld klicken um es zu bearbeiten. Durch einen Klick auf das **X** hinter einem Feld können Sie das Feld löschen. Es erscheint ein Dialog, in welchem Sie das Löschen noch kurz bestätigen müssen.

Benötigen Sie für diesen einen Datensatz ein weiteres Feld, so klicken Sie einfach auf **Feld hinzufügen** und im nächsten Dialog auf **Feld erstellen**. Im folgenden Screen können Sie das Feld an Ihre Anforderungen anpassen.

Löschen von Datensätzen

Um einen kompletten Datensatz zu löschen, klicken Sie einmal darauf um ihn auszuwählen. Anschließend können Sie – nach einem Klick auf den **Menübutton – Datensatz** löschen wählen. Es erscheint ein Dialog, in welchem Sie das Löschen noch kurz bestätigen müssen.

Passwort erzeugen

Sie können in der Password Safe App sichere Passwörter über den Passwortgenerator erzeugen lassen.

Öffnen Sie zunächst den entsprechenden Datensatz und klicken anschließend auf das **Stiftsymbol**.

Nun klicken Sie im Passwortfeld auf worauf sich der **Passwortgenerator** öffnet.

Sie sehen nun jeweils einen Schieberegler zum Bestimmen der Passwortlänge und einen für die Anzahl der Sicherheitspunkte. Durch Verschieben der Regler können Sie direkt mitverfolgen wie sich das Passwort ändert.

Ebenso können Sie festlegen, welche Art von Zeichen in das Passwort aufgenommen werden sollen.

Über einen Klick auf **OK** speichern Sie das erstellte Passwort abschließend ab.

Ordner

Was sind Ordner?

Innerhalb einer Datenbank können Sie verschiedene Ordner erstellen. Dies ermöglicht Ihnen die Passwörter zu sortieren und somit in einer übersichtlichen Struktur abzulegen. Sie können jedem Ordner ein sogenanntes Formular. Dieses bestimmt dann, welche Felder die Datensätze innerhalb eines Ordners beinhalten.

Standard Ordner

Um Ihnen den Einstieg in die Password Safe App zu erleichtern, sind standardmäßig folgende Ordner angelegt:

Kreditkarten	
Formular	Kreditkarte
Verwendung	Hier können Sie die Daten zu Ihren Kreditkarten ablegen
Felder	Karte
	Nummer
	Prüfnummer
	PIN
	Inhaber
	Gültig bis

Kundenkarten	
Formular	Kundenkarte
Verwendung	Hier können Sie Ihre Kundenkarten verwalten
Felder	Beschreibung
	Nummer
	Kundenportal
	URL
	Benutzername

	Passwort
	URL

Mobile Passwörter	
Formular	Mobiles Passwort
Verwendung	Hier können Sie Zugangsdaten für Webseiten ablegen
Felder	Beschreibung
	Benutzername
	Passwort
	URL

PINs	
Formular	PIN
Verwendung	Zum Verwalten von PINs
Felder	Beschreibung
	PIN

Erstellen von Ordnern

Sollten Sie weitere Ordner benötigen, klicken Sie in der **Ordnerübersicht** (Schlüsselsymbol) auf das **+** Symbol. Es öffnet sich ein Dialog, in welchem Sie auswählen, ob Sie ein Passwort oder einen Ordner erstellen möchten. Wählen Sie hier **Ordner erstellen**. Anschließend kommen Sie zu einem Screen in welchem die Eigenschaften des Ordners vergeben werden. Klicken Sie hier einfach in die betreffende Zeile um diese zu bearbeiten. Bestätigen Sie abschließend durch einen Klick auf **Speichern**.

Name: Geben Sie hier dem Ordner einen aussagekräftigen Namen.
Formular: Hier legen Sie fest, welches Formular neuen Ordner zugeordnet wird. Das Formular wiederum bestimmt, über welche Felder die Passwörter im Ordner verfügen.

Bearbeiten und Löschen von Ordnern

Soll ein Ordner umbenannt werden, so klicken Sie auf den entsprechenden Ordner. Anschließend klicken Sie auf den **Menübutton** und nun auf **Ordner anzeigen**. In dieser Ansicht können Sie über das **Stiftsymbol** den Ordnernamen bearbeiten oder auch ein anderes Formular zuweisen. Ebenso kann in dieser Ansicht – nach einem erneuten Klick auf den **Menübutton** – der Ordner gelöscht werden.

Formulare

Für was sind Formulare nötig?

- In den Formularen wird festgelegt, welche Felder Sie zum Anlegen eines Datensatzes zur Verfügung haben.
- Es gibt Standard Formulare, welche die meisten Anwendungsfälle abdecken und Ihnen somit den Einstieg in die Arbeit mit der Password Safe App erleichtern.
- Selbstverständlich können Sie die Standard Formulare an Ihre Bedürfnisse anpassen oder auch neue Formulare erstellen.

Beachten Sie bitte, dass die Formularverwaltung deaktiviert wird, sobald die mobile Datenbank mit einer Multiuser- oder Enterprise Server Datenbank synchronisiert wurde. Die Formulare werden dann über den PC Client verwaltet.

Erstellen von Formularen

Um ein neues Formular zu erstellen, klicken Sie zunächst auf den **Menübutton** und anschließend auf **Einstellungen**. Wählen Sie den Menüpunkt **Formular** unter **Allgemein**. Sie sind nun in der Formularverwaltung, in welcher Ihnen alle bestehenden Formulare angezeigt werden.

Nach einem Klick auf das **+** Symbol wird ein neues Formular erstellt. Vergeben Sie zunächst einen Namen für das Formular. Ein Klick in das Feld **Name** genügt, um das Formular benennen zu können. Sobald das geschehen ist, können Sie dem Formular die benötigten Felder zuweisen. Hierfür klicken Sie auf **Feld hinzufügen** am unteren Rand, um das Feld zu erstellen. Es erscheint ein Fenster, wo Sie das neue Feld konfigurieren können. Klicken Sie auf **Speichern**, um das Feld zu übernehmen. Sie können in die einzelnen Felder klicken, um diese anzupassen.

> Ein neu erstelltes Formular kann erst dann verwendet werden, wenn es einem Ordner zugewiesen wurde.

Bearbeiten von Formularen

Um ein neues Formular zu bearbeiten, klicken Sie zunächst auf den **Menübutton** und wählen dann Formulare. Sie sind nun in der Formularverwaltung, in welcher Ihnen alle bestehenden Formulare angezeigt werden. Hier klicken Sie auf das entsprechende Formular und anschließend anschließend auf das **Stiftsymbol**. Nun genügt ein Klick auf eines der Felder, um dieses zu ändern. Bestätigen Sie mit einem Klick auf **Speichern**. Durch einen Klick auf den **Menübutton** können Sie **Formular löschen** wählen. Es folgt ein Dialog in welchem das Löschen bestätigt werden muss.

Internet Browser

Aufrufen von Webseiten

Es gibt mehrere Möglichkeiten um gespeicherte Webseiten aufzurufen:

- Durch einen Klick auf vor einer URL
- Per Klick auf die URL bei geöffnetem Datensatz
- Über die Lesezeichen
- Über die Favoriten

Automatische Passworteintragung

Verwendung der automatischen Eintragung

Sofern eine Webseite über die Password Safe App aufgerufen wird, können Sie die entsprechenden Anmeldedaten automatisch eintragen lassen. Navigieren Sie hierzu (innerhalb der Password Safe App) zu der entsprechenden Webseite. Die Password Safe App analysiert nun die Webseite. Wird eine Loginmaske zweifelsfrei erkannt, werden Benutzername und Passwort automatisch eingetragen. Es reicht nun ein einfacher Klick auf den Loginbutton um sich anzumelden.

Einrichten der automatischen Eintragung (manuelles Anlernen)

Um zu verhindern, dass Ihre Daten an nicht dafür vorgesehene Felder übermittelt werden, müssen die Loginmasken zweifelsfrei als solche erkannt werden. Es kann daher vorkommen, bei einzelnen Webseiten die Daten nicht automatisch übermittelt werden. In solchen Fällen, können Sie die Webseiten jedoch manuell anlernen:

Legen Sie zunächst einen entsprechenden Datensatz an. Navigieren Sie nun zur entsprechenden Webseite.

Klicken Sie nun in der Loginmaske in das erste Feld. Es öffnet sich das Tastaturfeld über welchem die Feldliste eingeblendet wird. Hier wählen Sie – mittels der beiden Pfeiltasten – dasjenige Feld aus, welches Sie dem Feld in der Loginmaske zuordnen wollen. Dies könnte beispielsweise der Benutzername sein. Klicken Sie nun auf die Taste mit dem Feldnamen. Der Inhalt des Feldes wird nun in die Anmeldemaske übernommen. Sobald dies geschehen ist, wiederholen Sie den Vorgang mit dem nächsten Feld der Anmeldemaske, beispielsweise dem Passwortfeld. Die Zuordnungen werden automatisch abgespeichert. Beim nächsten Besuch der Website, wird nun die Loginmaske nach Ihren vorgaben befüllt. Sollte die Feldliste nicht zu sehen, beispielsweise weil die Zuordnung bereits erfolgte, so kann sie über den Menübutton eingeblendet werden.

Favoriten und Lesezeichen

Was sind Favoriten?

Passwörter können als Favoriten gekennzeichnet werden, um einen schnellen Zugriff zu ermöglichen. Hierbei haben Sie die Möglichkeit, **allgemeine Favoriten** und sogenannte **GeoFavs** zu erstellen. Allgemeine Favoriten sind überall verfügbar. Über die Funktion **GeoFav**, lassen sich Favoriten an einen Ort binden. Sie haben damit z.B. im Büro die Passwörter der Server und RDP Verbindungen zur Verfügung, während Sie Zuhause die Passwörter für Facebook und den privaten E-Mail-Account bequem und schnell auffinden können.

Die Favoritenverwaltung

Um die Favoritenverwaltung aufzurufen, klicken Sie einfach in der Toolbar auf **Favoriten**. In der Menüleiste können Sie dann zwischen **alle Favoriten** und den **GeoFavs** wählen.

Allgemeine Favoriten

Wie erstelle ich Favoriten?

Um einen Datensatz als Favorit zu kennzeichnen, muss dieser zunächst geöffnet werden. In der Menüleiste sehen Sie einen Stern. Ein einfacher Klick darauf, genügt um den Datensatz zu den Favoriten hinzuzufügen. Der Stern wird hierbei hervorgehoben.

Verwenden von Favoriten

Um einen Favoriten aufzurufen, klicken Sie in der Tab Bar auf . Es werden dann die Favoriten aufgelistet und können per Klick ausgewählt werden.

GeoFav

Was sind GeoFav

Über die Funktion **GeoFav**, lassen sich Favoriten an einen Ort binden. Sie haben damit z.B. im Büro die Passwörter der Server und RDP Verbindungen zur Verfügung, während Sie Zuhause die Passwörter für Facebook und den privaten E-Mail-Account bequem und schnell auffinden können.

Wie erstelle ich einen GeoFav

Um einen GeoFav zu erstellen, wählen Sie in der Favoritenübersicht zunächst einen allgemeinen Favoriten aus. Klicken Sie dann auf den **Menübutton** und anschließend auf **GeoFav** aktivieren. Der Favorit wird nun an den aktuellen Standort gebunden.

Lesezeichen

In den Lesezeichen werden alle Datensätze angezeigt, in welchen sich eine URL befindet. Über einen Klick auf kann die Übersicht aufgerufen werden. Über einen einfachen Klick auf einen der Datensätze, wird die entsprechende Webseite aufgerufen.

Synchronisierung

WLAN Synchronisation

Voraussetzungen

Bevor Sie mit der Synchronisierung starten stellen Sie bitte folgendes sicher:

- Auf dem PC muss Password Safe 7 (Standard Edition oder höher) installiert sein
- Auf dem PC muss eine Datenbank erstellt sein
- Die Password Safe App muss auf Ihrem mobilen Gerät installiert sein
- Das Smartphone bzw. Tablet muss sich über WLAN im gleichen Netzwerk wie der PC befinden, alle Geräte müssen untereinander kommunizieren dürfen
- Der Port 11001 TCP muss in allen Firewalls freigegeben sein

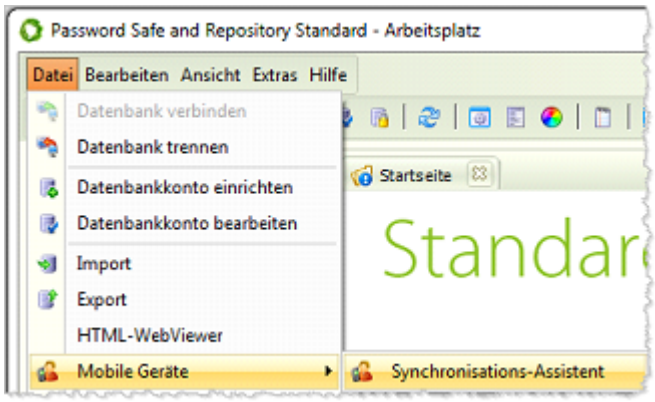
> Bitte beachten Sie, dass die Namen und Passwörter der Datenbanken nicht zwingend übereinstimmen müssen

Freigeben der Synchronisation (Multiuser- und Enterprise Server Datenbanken)

Sollten Sie eine Multiuser- oder Enterprise Server Datenbank verwenden, müssen Sie den Sync zunächst unter **Bearbeiten -> Datenbank Einstellungen -> mobile Geräte** freigeben. Weitere Informationen dazu finden Sie in der Hilfe des PC Clients.

Vorbereitung des Password Safe Clients

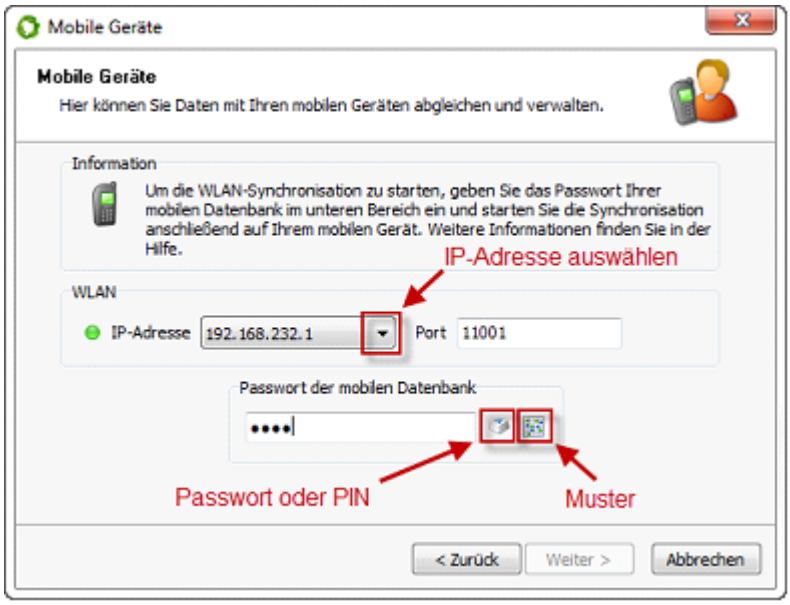
Die Synchronisierung muss zunächst am Password Safe Client vorbereitet werden. Gehen Sie hierfür auf **Datei -> Mobile Geräte -> Synchronisations-Assistent**:



Anschließend wählen Sie **WLAN Synchronisation** und bestätigten mit Weiter:

Mobile Geräte
Mobile Geräte
Hier können Sie Daten mit Ihren mobilen Geräten abgleichen und verwalten.
Wählen Sie bitte, wie die Daten Ihrer mobilen Datenbank verarbeitet werden sollen. Beachten Sie, dass eine direkte WLAN-Synchronisation nur möglich ist, wenn Ihr mobiles Gerät sich im selben Netzwerk wie der Client befindet, auf welchem Password Safe installiert ist.
WLAN Synchronisation
Mobile Datenbank mit Password Safe synchronisieren
Manuelle Synchronisation
Sicherung (.psmobile) mit Password Safe synchronisieren
Bei dieser Synchronisation wird die Password Safe Datenbank mit einer Sicherung Ihres mobilen Geräts (.psmobile) abgeglichen. Diese kann im Anschluss dann wieder auf das mobile Gerät aufgespielt werden.
< Zurück
Weiter >
Abbrechen

Im nächsten Fenster wählen Sie bitte diejenige IP-Adresse aus, über welche Ihr PC im Netzwerk eingebunden ist. Sollte Ihr PC nur einen Netzwerkadapter haben, kann die IP-Adresse nicht geändert werden. Sollten Sie nicht wissen, welche IP-Adresse die richtige ist, können Sie dies einfach ausprobieren. Nun geben Sie bitte noch das Passwort bzw. die PIN der mobilen Datenbank an. Sollte Sie die mobile Datenbank mit einem Muster geschützt haben, können Sie über die entsprechende Schaltfläche die Ansicht umschalten und auch am PC ein Muster eingeben:


Mobile Geräte
Mobile Geräte
Hier können Sie Daten mit Ihren mobilen Geräten abgleichen und verwalten.
Information
Um die WLAN-Synchronisation zu starten, geben Sie das Passwort Ihrer mobilen Datenbank im unteren Bereich ein und starten Sie die Synchronisation anschließend auf Ihrem mobilen Gerät. Weitere Informationen finden Sie in der Hilfe.
IP-Adresse auswählen
WLAN
IP-Adresse
192.168.232.1
Port
11001
Passwort der mobilen Datenbank
Passwort oder PIN
Muster
< Zurück
Weiter >
Abbrechen

Beachten Sie bitte, dass die **Weiter** Schaltfläche weiterhin ausgegraut bleibt. Der Password Safe Client ist nun fertig vorbereitet. Belassen Sie bitte den PC unbedingt in dieser Ansicht. Alle weiteren Schritte werden nun direkt an Ihrem Smartphone oder Tablet durchgeführt.

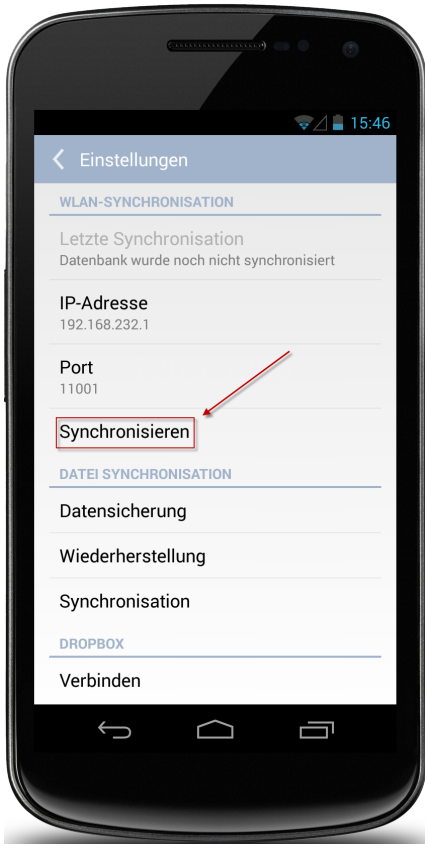
Vorbereiten und Start der Synchronisierung am Smartphone / Tablet

Melden Sie sich zunächst an Ihrer mobilen Datenbank an:

Öffnen Sie nun die **Einstellungen**:

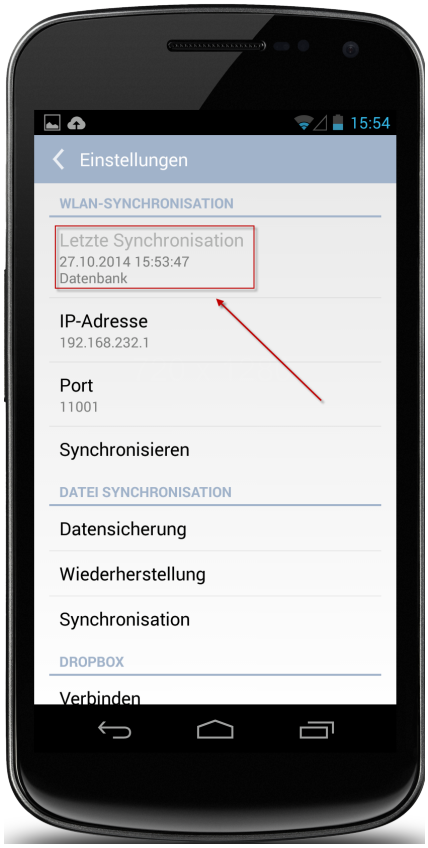
Nun scrollen Sie zum Punkt **WLAN Synchronisation**. Klicken Sie in das leere Feld unter **IP Adresse** und tragen dort diejenige IP Adresse ein, welche Sie am PC angezeigt bekommen bzw. ausgewählt haben. Klicken Sie auf OK. (Beachten Sie bitte, dass auf manchen Geräten nach jedem Punkt automatisch ein Leerzeichen eingefügt wird. Diese müssen manuell entfernt werden!) Prüfen Sie auch ob der Port an beiden Geräten übereinstimmt:

Nun klicken Sie am Handy auf Synchronisieren:



Es öffnet sich ein neuer Screen, in welchem Sie nun die Synchronisation starten:

Sobald die Synchronisation abgeschlossen ist klicken Sie auf die Zurück Schaltfläche. Es werden Ihnen die Informationen zur letzten Datenübertragung angezeigt:



Abschließend klicken Sie am PC auf Fertigstellen zum Beenden:

Mobile Geräte
Mobile Geräte
Hier können Sie Daten mit Ihren mobilen Geräten abgleichen und verwalten.
Die Synchronisation ist abgeschlossen. Prüfen Sie nun die Daten auf Ihrem mobilen Gerät.
< Zurück
Weiter >
Fertigstellen

Google Drive Synchronisation / Backup

Es besteht die Möglichkeit ein Backup Ihrer mobilen Datenbank direkt in Google Drive abzulegen, um Ihre Datenbank zu sichern. Ebenso kann eine Synchronisationsdatei zum Abgleich der Daten zwischen einem Password Safe Client und mobilem Gerät erstellt und damit synchronisiert werden.

Voraussetzungen

Bevor Sie Ihre Daten synchronisieren, stellen Sie bitte sicher, dass folgende Voraussetzungen gegeben sind:

- Auf dem Client muss eine lauffähige Datenbank eingebunden sein.
- In der Password Safe App muss ebenfalls eine lauffähige Datenbank existieren.
- Ein Google Drive Account muss vorhanden und sowohl vom Client als auch vom mobilen Gerät aus verfügbar sein.

Verbinden / Trennen mit Google Drive

Zunächst muss sichergestellt sein, dass eine Verbindung zu Google Drive besteht. Navigieren Sie zu den **Einstellungen** und scrollen dann zu **Google Drive**. Klicken Sie hier auf **Verbinden** und wählen Sie anschließend das gewünschte Konto aus und bestätigen mit **OK**. Sobald Sie mit Google Drive verbunden sind, wechselt der Menüpunkt zu **Verbindung trennen** und weitere Menüpunkte werden eingeblendet. Ein Klick auf Verbindung trennen reicht aus, um die Verbindung zu Google Drive zu beenden.

Beim ersten Verbindungsaufbau wird die Password Safe App in der Google Drive initialisiert und folgender Ordner angelegt:
…\Password Safe and Repository\

Erstellen einer Datensicherung (Backup)

Es wird immer empfohlen ein Backup zu erstellen, um Ihre Daten zu sichern. In den **Einstellungen** finden Sie unter **Google Drive** den Punkt **Datensicherung**. Klicken Sie einfach darauf und anschließend auf **Start**. In **Google Drive** wird nun eine Backupdatei erstellt, welche jederzeit an einem mobilen Gerät zurück gespielt werden kann.

Der Name der Backupdatei setzt sich wie folgt zusammen: Gerät_Datenbankname_DatumUhrzeit.psmobile
Beispiel: Smartphone_Meine-Datenbank_18032012172310.psmobile

Rückspielen einer Datensicherung (Backup Restore)

Nach dem Anmelden an der Datenbank wechseln Sie zu den **Einstellungen -> Google Drive -> Wiederherstellung**. Es wird nun der Google Drive Ordner "…\Password Safe and Repository\" nach Backups durchsucht. Wählen Sie nun einfach das gewünschte Backup aus und bestätigen mit einem Klick auf **Start**.

Sollten sich in Ihrer mobilen Datenbank Daten befinden, werden diese zunächst gelöscht. Anschließend wird die Datenbank mit den Daten aus dem Backup befüllt.

Beachten Sie bitte, dass das Datenbankpasswort beim Restore mit dem Datenbankpasswort des Backups übereinstimmen muss.

Synchronisation

Die Daten Ihrer Password Safe App sowie Ihres Password Safe Clients können mit einer sogenannten Synchronisationsdatei über Goolge Drive abgeglichen werden. Dies kann sowohl vom Password Safe Client als auch vom mobilen Gerät aus geschehen. Bitte schließen Sie eine Synchronisation immer komplett ab, bevor Sie mit einem anderen Gerät ebenfalls eine Synchronisation starten.

Mobiles Gerät

Um vom Smartphone bzw. Tablet aus zu synchronisieren, navigieren Sie hierfür einfach zu **Einstellungen -> Google Drive** und klicken dann auf **Synchronisation**. Beim ersten Synchronisieren wird im Ordner …\Password Safe and Repository\ eine entsprechende Synchronisationsdatei erstellt. Bei zukünftigen Synchronisationen werden die Daten mit der bestehenden Datei abgeglichen.

Der Name der Synchronisationsdatei setzt sich wie folgt zusammen:
sync_Datenbankname_Hashwert.psmobile
Beispiel: sync_Meine-Datenbank_8595cc75d296ac14768ca4d554ea4d63.psmobile

Client

Zur ersten Synchronisation mit dem Password Safe Client muss zunächst die entsprechende Synchronisationsdatei ausgewählt werden. Hierzu wechseln Sie zu **Datei -> Mobile Geräte -> Synchronisations-Assistent** und wählen dort **manuelle Synchronisation**. Im nächsten Schritt können Sie den Menüpunkt **mit bestehender Synchronisationsdatei abgleichen** bestätigen und die entsprechende

Synchronisationsdatei auswählen. Nach einem Klick auf **Weiter** muss dann lediglich noch das Passwort der mobilen Datenbank eingegeben und bestätigt werden. Nun können Sie den Assistenten fertigstellen und die Synchronisation beginnt.

Vorausgesetzt, dass eine gültige Synchronisationsdatei bereits erstellt und über den Assistenten eingebunden wurde, können Sie komfortabel damit synchronisieren. Hierfür wird der Menüpunkt **Datei -> Mobile Geräte -> Synchronisieren** eingeblendet. Ein einfacher Klick darauf genügt, um die Synchronisation zu starten.

Erstellen einer Synchronisationsdatei am Password Safe Client

Auch am Password Safe Client kann eine neue Synchronistationsdatei erstellt werden. Im Gegensatz zur Password Safe App, geschieht dies jedoch manuell.

Über **Datei -> Mobile Geräte -> Assistent** starten Sie den Synchronisationsassistenten. Wählen Sie hier zunächst **manuelle Synchronisation** und bestätigen mit einem Klick auf **Weiter**.

Im nächsten Schritt wählen Sie bitte **Neue Synchronisationsdatei** erstellen und vergeben einen Namen für die Datei. Zudem wählen Sie den gewünschten Speicherort aus. Bestätigen Sie mit **Weiter**.

> Möchten Sie von einem mobilen Gerät aus die Datei synchronisieren, muss folgender Speicherort gewählt werden:
> …\Google Drive\Password Safe and Repository\
> Der Name der Synchronisationsdatei muss dem Namen der mobilen Datenbank entsprechen.

Nun muss noch das Passwort der mobilen Datenbank (mit welcher später synchronisiert werden soll) angegeben und mit **Weiter** bestätigt werden. Nach einem Klick auf **Fertigstellen** wird die Synchronisationsdatei erzeugt.

Dropbox Synchronisation / Datensicherung

Es besteht die Möglichkeit ein Backup Ihrer mobilen Datenbank direkt in der Dropbox abzulegen um Ihre Datenbank zu sichern. Ebenso kann eine Synchronisationsdatei zum Abgleich der Daten zwischen einem Password Safe Client und mobilem Gerät erstellt und damit synchronisiert werden.

Voraussetzungen

Bevor Sie Ihre Daten synchronisieren, stellen Sie bitte sicher, dass folgende Voraussetzungen gegeben sind:

- Auf dem Client muss eine lauffähige Datenbank eingebunden sein.
- In der Password Safe App muss ebenfalls eine lauffähige Datenbank existieren.
- Ein Dropbox Account muss vorhanden und sowohl vom Client als auch vom mobilen Gerät aus, verfügbar sein.

Verbinden / Trennen mit der Dropbox

Zunächst muss sichergestellt sein, dass eine Verbindung zur Dropbox besteht. Navigieren Sie zu den **Einstellungen** und scrollen dann zu **Dropbox**. Klicken Sie hier auf **Verbinden** und folgen dann dem Dialog der Dropbox. Sobald Sie mit der Dropbox verbunden sind, wechselt der Menüpunkt zu **Verbindung trennen** und weitere Menüpunkte werden eingeblendet. Ein Klick auf **Verbindung trennen** reicht aus, um die Verbindung zur Dropbox zu beenden.

Beim ersten Verbindungsaufbau zur Dropbox wird die Password Safe App in der Dropbox initialisiert und folgender Ordner angelegt:

- ..\Dropbox\Apps\Password Safe Mobile*

Erstellen einer Datensicherung (Backup)

Es wird empfohlen ein Backup zu erstellen um Ihre Daten zu sichern. In den **Einstellungen** finden Sie unter **Dropbox** den Punkt **Datensicherung**. Klicken Sie einfach darauf und anschließend auf **Start**. In Ihrer Dropbox wird nun eine Backupdatei erstellt, welche jederzeit an einem mobilen Gerät zurück gespielt werden kann.

Der Name der Backupdatei setzt sich wie folgt zusammen: Gerät_Datenbankname_DatumUhrzeit.psmobile
Beispiel: Smartphone_Meine-Datenbank_18032012172310.psmobile

Rückspielen einer Datensicherung (Backup Restore)

Nach dem Anmelden an der Datenbank wechseln Sie zu den **Einstellungen -> Dropbox -> Wiederherstellung**. Es wird nun in Ihrer Dropbox der Ordner "…\Dropbox\Apps\Password Safe Mobile\" nach Backups durchsucht. Wählen Sie nun einfach das gewünschte Backup aus und bestätigen mit **Sicherung einspielen**.

Sollten sich in Ihrer mobilen Datenbank Daten befinden, werden diese zunächst gelöscht. Anschließend wird die Datenbank mit den Daten aus dem Backup befüllt.

Beachten Sie bitte, dass beim Restore auch das ursprüngliche Datenbankpasswort mit eingespielt wird. Nach dem Rückspielen des Backups müssen Sie sich also mit dem Datenbankpasswort anmelden, welches zum Zeitpunkt der Erstellung des Backups gültig war.

Synchronisation

Die Daten Ihrer Password Safe App sowie Ihres Password Safe Clients können mit einer sogenannten Synchronisationsdatei in Ihrer Dropbox abgeglichen werden. Dies kann sowohl vom Password Safe Client als auch vom mobilen Gerät aus geschehen. Bitte schließen Sie eine Synchronisation immer komplett ab, bevor Sie mit einem anderen Gerät ebenfalls eine Synchronisation starten.

Mobiles Gerät

Um vom Smartphone bzw. Tablet aus zu synchronisieren, navigieren Sie hierfür einfach zu **Einstellungen -> Dropbox** und klicken dann auf **Synchronisation**. Beim ersten Synchronisieren wird im Ordner …\Dropbox\Apps\Password Safe Mobile\ eine entsprechende Synchronisationsdatei erstellt. Bei zukünftigen Synchronisationen werden die Daten mit der bestehenden Datei abgeglichen.

Der Name der Synchronisationsdatei setzt sich wie folgt zusammen:
sync_Datenbankname_Hashwert.psmobile
Beispiel: sync_Meine-Datenbank_8595cc75d296ac14768ca4d554ea4d63.psmobile

Client

Zur ersten Synchronisation mit dem Password Safe Client muss zunächst die entsprechende Synchronisationsdatei ausgewählt werden. Hierzu wechseln Sie zu **Datei -> Mobile Geräte -> Synchronisations-Assistent** und wählen dort **manuelle Synchronisation**. Im nächsten Schritt können Sie **mit bestehender Synchronisationsdatei abgleichen** aktivieren und die entsprechende Synchronisationsdatei in Ihrer Dropbox auswählen. Nach einem Klick auf **Weiter** muss dann lediglich noch das Passwort der mobilen Datenbank eingegeben und bestätigt werden. Nun können Sie den Assistenten fertigstellen und die Synchronisation beginnt.

Vorausgesetzt, dass eine gültige Synchronisationsdatei bereits erstellt und über den Assistenten eingebunden wurde, können Sie komfortabel damit synchronisieren. Hierfür wird der Menüpunkt **Datei -> Mobile Geräte -> Synchronisieren** eingeblendet. Ein einfacher Klick darauf genügt, um die Synchronisation zu starten.

Erstellen einer Synchronisationsdatei am Password Safe Client

Auch am Password Safe Client kann eine neue Synchronistationsdatei erstellt werden. Im Gegensatz zur Password Safe App, geschieht dies jedoch manuell.

Über **Datei -> Mobile Geräte -> Assistent** starten Sie den Synchronisationsassistenten. Wählen Sie hier zunächst **manuelle Synchronisation** und bestätigen mit einem Klick auf **Weiter**.

Im nächsten Schritt wählen Sie bitte **Neue Synchronisationsdatei** erstellen und vergeben einen Namen für die Datei. Zudem wählen Sie den gewünschten Speicherort aus. Bestätigen Sie mit **Weiter**.

> Möchten Sie von einem mobilen Gerät aus die Datei synchronisieren, muss folgender Speicherort gewählt werden:
> …\Dropbox\Apps\Password Safe Mobile\
> Der Name der Synchronisationsdatei muss dem Namen der mobilen Datenbank entsprechen.

Nun muss noch das Passwort der mobilen Datenbank (mit welcher später synchronisiert werden soll) angegeben und mit Weiter bestätigt werden. Nach einem Klick auf Fertigstellen wird die Synchronisationsdatei erzeugt.

Airpass

Sofern Sie sich mit Ihrem Smartphone in einem WLAN Netz befinden, können die einzelne Daten aus der Password Safe App per WLAN in einer verschlüsselten HTML-Datei bereitgestellt werden. Auf diese kann mit jedem handelsüblichen Browser zugegriffen werden. Somit haben Sie die Möglichkeit, Ihre Passwörter auf einem PC oder auch einem anderen Smartphone einzusehen. Beachten Sie bitte, dass diese Option über den Client deaktiviert werden kann.

Bereitstellung

Um AirPass zu starten, klicken Sie innerhalb eines Passwort-Datensatzes auf den **Menübutton** und **mit airPass bereitstellen**. Anschließend wird eine hochverschlüsselte HTML-Datei erstellt. Diese wird unter der IP-Adresse des Smartphones im Netzwerk bereitgestellt. Um die Datei von einem PC aus aufzurufen reicht es aus, die IP-Adresse inkl. dem Port, welche auf dem Smartphone angezeigt wird, in den Browser einzugeben.

Bedienung

Nachdem Sie AirPass am Browser geöffnet haben, erhalten Sie eine Anmeldemaske. Es wird Ihnen der Datenbankname und der Name Ihres Smartphones angezeigt.

Nachdem Sie im Passwortfeld Ihr persönliches Passwort eingegeben haben, können Sie die WebViewer-Datei über einen Klick auf **Anmelden** öffnen.

Im Hauptfenster wird Ihnen oben der Datenbankname angezeigt. Daneben läuft ein Timer. Dieser startet bei 60 Sekunden und zählt auf 0 herunter. Danach wird die Datei aus Sicherheitsgründen wieder gesperrt. Nach jeder Eingabe startet der Timer erneut.

In der Zeile darunter sehen Sie ein Suchfenster und den dazugehörigen Button **Suchen**. Durch einen einfachen Klick auf **Suchen**, wird Ihnen nun der Datensatz angezeigt. Klicken Sie auf ein Passwort, wird dieses für 10 Sekunden im Klartext dargestellt und anschließend wieder verschlüsselt.

Beachten Sie bitte, dass Sie Sie auf die zur Verfügung gestellte URL aus Sicherheitsgründen nur einmal zugreifen können. Die Datei wird also nach dem Zugriff direkt wieder gelöscht. Selbstverständlich kann die Datei (wie oben beschrieben) jederzeit wieder erzeugt werden.

Einstellungen

Datenbankeinstellungen

In diesem Abschnitt können Sie alle relevanten Informationen Ihrer Datenbank einsehen bzw. ändern.

- **Datenbank Name:** Über einen Klick kann der Name der Datenbank geändert werden.
- **Login Versuche:** Legen Sie hier fest, nach wie vielen gescheiterten Anmeldeversuchen die Datenbank gelöscht wird.
- **Ablaufdatum:** Zu diesem Datum wird die Datenbank automatisch gelöscht.
- **Passwort ändern:** Vergeben Sie hier ein neues Passwort für die Datenbank.

Sicherheitseinstellungen

Unter dem Menüpunkt **Sicherheit** können Sie folgende Optionen aktivieren bzw. deaktivieren:

- **Automatisch sperren:** Diese Option bewirkt, dass die Password Safe App gesperrt wird, wenn Sie entweder Ihr mobiles Gerät sperren oder zu einer anderen App wechseln.
- **Datenbank sperren (sek):** Hier können Sie festlegen, nach wie viel Sekunden die Datenbank gesperrt wird. Bei “0” erfolgt die Sperre ohne Zeitversatz.
- **Zwischenablage leeren (sek):** Stellen Sie hier ein, wie lange die Password Safe App App Daten in der Zwischenablage belässt, bevor diese geleert wird.

- **Browser Autofill:** Legen Sie hier fest, ob Zugangsdaten automatisch in die entsprechenden Loginfelder von Webseiten eingetragen werden, oder nicht.
- **airpass Port:** Hier kann der Port über welchen airpass Daten bereitstellt angepasst werden.

Allgemeine Einstellungen

Unter **Allgemein** können Sie folgende Punkte konfigurieren:

- **Formulare:** Verwalten Sie hier die Formulare der mobilen Datenbank. Weitere Informationen finden Sie im Kapitel Formulare.
- **Hilfe:** Hier können Sie sich die Onlinehilfe anzeigen lassen.

Info

In dieser Ansicht können Sie sich folgende Informationen ansehen:

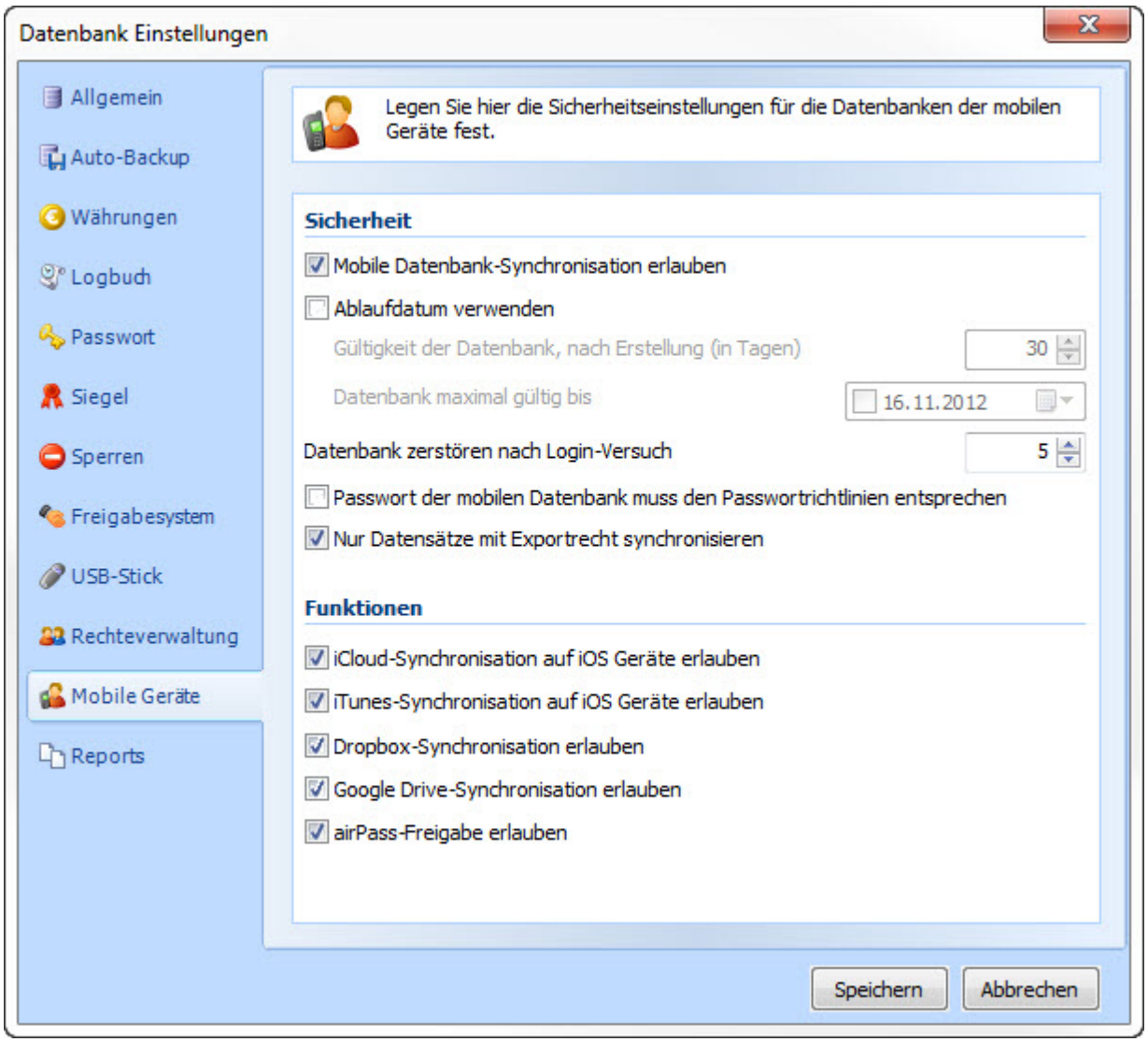
- **Gutschein anzeigen:** Mit der Password Safe App erhalten Sie einen Gutschein über welchen Sie den Password Safe PC Client in der Standard Edition 25% günstiger erhalten. Sollten Sie den Gutschein ausgeblendet haben und dennoch nutzen wollen, so können Sie in hier wieder anzeigen lassen.
- **Lizenzbestimmungen:** Hier können Sie die Lizenzbestimmungen abrufen.

Sollten Sie einen Teil dieser Optionen vermissen, so wurde Ihre mobile Datenbank mit einer Multiuser oder Enterprise Server Datenbank synchronisiert. In diesem Fall werden die entsprechenden Einstellungen am Password Safe Client vorgenommen, bzw. vom Administrator vorgegeben.

Einstellungen am Password Safe Client

In Multiuser- oder Enterprise Server Datenbanken werden diverse Einstellungen bzgl. der Password Safe App direkt am Password Safe Client vorgenommen. Diese finden Sie unter **Bearbeiten -> Datenbank Einstellungen -> Mobile Geräte**.

> Dieser Dialog ist nur in Verbindung mit Multiuser bzw. Enterprise Server Datenbanken ab der Professional Edition verfügbar. In der Standard Edition ist er nicht nötig. Die Synchronisierung ist dennoch möglich.



Sicherheit:

- **Mobile Datenbank-Synchronisation erlauben:** Durch diese Option kann erlaubt bzw. verhindert werden, dass die lokale Datenbank mit mobilen Geräten abgeglichen wird.
- **Ablaufdatum verwenden:** Legen Sie hier fest, wie lange bzw. bis zu welchem Datum die mobile Datenbank verwendet werden kann, bis Sie zerstört wird.
- **Passwort der mobilen Datenbank muss den Passwortrichtlinien entsprechen:** Hier kann die Verwendung von leicht knackbaren Passwörtern verhindert werden.
- **Nur Datensätze mit Exportrecht synchronisieren:** Datensätze, auf welche der Benutzer kein Exportrecht hat, werden nicht synchronisiert

Funktionen:

- **iCloud-Synchronistaion auf iOS Geräte erlauben:** Geben Sie die mobile Datenbank zum Abgleich mit der iCloud frei. (Nur bei Verwendung von iOS möglich)
- **iTunes-Synchronisation auf iOS Geräte erlauben.** Erlauben Sie hier den Abgleich über iTunes (Nur bei Verwendung von iOS möglich)
- **Dropbox-Synchronistaion erlauben:** Geben Sie die mobile Datenbank zum Abgleich mit der Dropbox frei. (iOS und Android)
- **Google Drive-Sycnhronisation erlauben:** Erlauben Sie hier den Abgleich über Google Drive (Nur bei Verwendung von Windows Phone)
- **airPass-Freigabe erlauben:** Ermöglicht dem Benutzer einzelne Datensätze per AirPass über WLAN zur Verfügung zu stellen.

Support

Nehmen Sie Kontakt mit uns auf…

MATESO GmbH
Daimlerstraße 7
86368 Gersthofen
Deutschland

Telefon Hotline:

Deutschland: +49 900 5225562
(1,99 € / Min. aus dem dt. Festnetz)

Österreich: +43 900 511503
(2,16 € / Min. aus dem österr. Festnetz)

Schweiz: +41 900 807020
(2,50 SFR / Min. aus dem schw. Festnetz)

Mo. bis Do. 9-17 Uhr, Fr. von 9-15 Uhr

E-Mail:

support@passwordsafe.de

Support (technischer Support und Kundendienst)

Wenn Sie Support benötigen, dazu zählen auch Fragen zur Bedienung der Software, so wenden Sie sich bitte telefonisch an die Hotline, oder benutzen Sie unser Forum. Alternativ können Sie auch eine Email an support@passwordsafe.de senden oder unser Supportformular benutzen.

Lizenzbestimmungen

Lizenzbestimmungen für Software der MATESO GmbH

für in Deutschland erworbene Password Safe Lizenzen

Stand April 2013

1.Allgemeiner Geltungsbereich

1.1 Diese Lizenzbestimmungen gelten ergänzend zu den Allgemeinen Geschäftsbedingungen der MATESO GmbH (nachstehend Lizenzgeber). Diese Bestimmungen gelten neben der gelieferten Software auch für alle Updates, Upgrades, Ergänzungen, den Support und sonstige über das Internet angebotene Dienste. Sollten insoweit den oben genannten Produkten eigene Lizenzbestimmungen beiliegen, gelten diese vorrangig.

1.2 Indem der Lizenznehmer die Software installiert bzw. benutzt, erkennt er diese Lizenzbestimmungen an.

1.3 Wurde die Software von einem Vertriebspartner (cleverbridge) erworben, gelten die gesamten Lizenzbedingungen und bleiben unberührt. Das Nutzungsrecht wird ausschließlich von MATESO in dem in diesen Lizenzbestimmungen bestimmten Umfang eingeräumt.

1.4 Die Systemverantwortung liegt beim Lizenznehmer. Der Lizenzgeber schuldet im Wege des Direktvertriebs nur die Lieferung der Software. Als Lieferung der Software wird insbesondere die Downloadmöglichkeit angesehen.

2.Definitionen

2.1 Lizenzprodukte sind alle von der MATESO GmbH angebotenen Softwareprodukte.

2.2 Zum Lizenzmaterial gehören auch die Updates und Dokumentationen, die der Lizenzgeber dem Lizenznehmer überlässt.

3.Rechteverteilung

3.1 Der Lizenzgeber bleibt Inhaber aller Rechte am Lizenzprodukt, auch wenn der Lizenznehmer das Lizenzprodukt unberechtigterweise verändert oder mit seinen eigenen Programmen oder denjenigen eines Dritten verbindet. Dies gilt auch, wenn der Reseller den Lizenzschlüssel auf einen anderen Namen als auf MATESO ausstellt. Hiervon ausgenommen ist die Rechtseinräumung nach diesen Bestimmungen.

3.2 Der Lizenzgeber räumt dem Lizenznehmer ein nicht ausschließliches, nicht unterlizensierbares einfaches Nutzungsrecht an den Lizenzprodukten und der Dokumentation ein.

3.3 Ausschließlich zu Sicherungszwecken ist der Lizenznehmer berechtigt, Kopien des überlassenen Lizenzproduktes herzustellen. Der Lizenzgeber erwirbt an diesen Kopien sämtliche Rechte, sofern sie nicht durch diese Bestimmungen auf den Lizenznehmer übertragen wurden. Der Lizenznehmer ist berechtigt, die Lizenzprodukte im Rahmen der bestimmungsgemäßen Verwendung auf seiner DV-Anlage zu nutzen, auch wenn hierbei im Arbeitsspeicher Zwischenkopien angefertigt werden. Die Herstellung weiterer Kopien ist nicht gestattet.

3.4 Soweit die Veräußerung der Lizenz an Dritte nach dem maßgebenden Landesrecht beziehungsweise der Rechtsprechung möglich ist, ist der ursprüngliche Lizenznehmer verpflichtet, die auf seine DV-Anlage heruntergeladene Kopie zum Zeitpunkt des Weiterverkaufs vollständig unbrauchbar zu machen. Eine weitere Nutzung durch den ursprünglichen Lizenznehmer stellt einen Verstoß gegen das ausschließliche Vervielfältigungsrecht des Lizenzgebers dar und wird zivil- und strafrechtlich verfolgt.

3.5 Einzelne Editionen mit mehreren Lizenzen dürfen nicht aufgespalten und einzeln verkauft werden.

3.6 Eine Weitergabe der Software und Lizenzen durch Verkauf ist grundsätzlich erst nach Lizenzumschreibung durch MATESO möglich. Eine Lizenzumschreibung aufgrund eines Verkaufs durch den ursprünglichen Lizenznehmer, eine Lizenzänderung und eine erneute Lizenzausstellung sind nur gegen Entrichtung einer Gebühr an MATESO möglich.

4.Besondere Bestimmungen zum Nutzungsrecht an den Vollversionen

4.1 Der Lizenznehmer ist berechtigt, die Software in der entsprechend erworbenen Anzahl von Lizenzen zu nutzen. Es handelt sich hierbei um ein sog. Named-User-Lizenzmodell.

4.2 Durch den Erwerb einer Lizenz ist jeweils ein Lizenznehmer berechtigt, die Software zu installieren und zu nutzen. Die Datenbank kann von allen named usern benutzt werden.

4.3 Die Software darf nur auf einem PC installiert und genutzt werden. Soll die Software auf einem anderen PC oder DV-Anlage installiert werden, ist die Software vom Erstgerät vollständig zu deinstallieren. Eine Mehrfachinstallation ist erst nach Entrichtung einer Gebühr zulässig.

4.4 Für die Speicherung der Software auf einer Datenverarbeitungseinheit, die als Server benutzt wird, bedarf es des Erwerbs einer Serverlizenz (Terminalserver/Citrix Modul). Einzellizenzen dürfen dort nicht installiert werden.

4.5 Darüber hinaus muss bei der Verwendung der Lizenzen auf einem Server sichergestellt sein, dass für jeden Nutzer eine eigene Lizenz erworben wurde.

5.Besondere Bestimmungen zum Nutzungsrecht an der Demoversion (Testphase)

5.1 Die Lizensierung auf Testbasis ist möglich. Die Nutzungsrechte an der Demoversion der Software sind zeitlich auf die Testphase (30 Tage) beschränkt. Es handelt sich dabei um ein nicht ausschließliches, nicht unterlizensierbares, zeitlich beschränktes einfaches Nutzungsrecht.

5.2 Während der Testphase ist der Lizenznehmer berechtigt, anderen PC-Anwendern die Demosoftware zu Testzwecken zur Verfügung zu stellen. Stellt der Lizenznehmer die Demosoftware anderen Anwendern zur Verfügung, ist er verpflichtet, diese auf die Testlaufzeit und die Folgen bei Nutzung der Software nach Ablauf der Testphase hinzuweisen. Der Lizenznehmer ist für die Einhaltung dieser und der gesetzlichen Bestimmungen auch im Hinblick auf die Verwendung durch Dritte verantwortlich.

5.3 Nach Ablauf der Testphase stellt das weitere Verwenden der Demosoftware eine strafbare Urheberrechtsverletzung dar, deren Verfolgung sich der Lizenzgeber ausdrücklich vorbehält.

5.4 Nach Ablauf der Testphase kann die Software durch einen Lizenzschlüssel freigeschalten werden. Dadurch erhält der Lizenznehmer ein Nutzungsrecht in dem in diesen Lizenzbestimmungen beschriebenen Umfang. Der Nutzungsumfang der Vollversion richtet sich neben den anderen Bestimmungen insbesondere nach Nr. 3 dieser Lizenzbestimmungen.

6.Bearbeitung, Reverse Engineering

6.1 Dem Lizenznehmer ist es nicht gestattet, die Software in irgendeiner Form zu bearbeiten, zu vervielfältigen oder zu übersetzen. Jegliche Form des Reverse Engineering ist untersagt. Dazu gehört unter anderem das Extrahieren von Konstruktionselementen des Lizenzprodukts oder Teile davon. Weiter ist es dem Lizenznehmer untersagt den ursprünglichen Quellcode zu erzeugen (dekompilieren) oder die Software zu disassemblieren (Umwandlung der Maschinensprache in eine für Menschen lesbare Assemblersprache). Eine Ausnahme gilt nur für den Fall, dass die Dekompilierung der Software zur Ermittlung von Schnittstelleninformationen zwingend erforderlich ist und MATESO nach schriftlicher Aufforderung durch den Lizenznehmer die erforderlichen Informationen für die Interoperabilität nicht ohne weiteres zugänglich gemacht hat.

6.2 §§ 69d Abs. 2 und 3 und 69e UrhG bleiben unberührt.

7. Dokumentation

Die Dokumentation (Benutzerhandbuch) steht auf der Internetseite www.passwordsafe.de unter der Rubrik Support im Download Center in ausdruckbarer Form als PDF-Datei zur Verfügung.

8. Softwarepflege und Support

8.1 Der Lizenznehmer kann zwischen verschiedenen Ausgestaltungen der Softwarepflege und des Supports wählen. Je nach Auswahl (Private, Company Classic, Company Premium) richtet sich das Nutzungsrecht an den Updates etc.

8.2 Das Nutzungsrecht an der primär erworbenen Software erlischt nicht durch Ablauf des Softwarepflegezeitraums. Die ursprünglich erworbene Software kann in dem oben beschriebenen Maße weiter benutzt werden, jedoch sind ohne Verlängerung der Softwarepflege keine Updates, Upgrades oder Support mehr möglich.

8.3 Der Lizenznehmer erhält im Rahmen der Softwarepflege für 12 Monate ein nicht ausschließliches, nicht übertragbares, nicht unterlizensierbares einfaches Nutzungsrecht an den Softwarepflegeprodukten. Die Softwarepflege kann nicht unterbrochen werden.

8.4 30 Tage vor Ablauf des Softwarepflegezeitraums kann der Lizenznehmer die Softwarepflege verlängern. Verlängert der Lizenznehmer die Softwarepflege, erhält er wieder für 12 Monate ein nicht ausschließliches, nicht übertragbares, nicht unterlizensierbares einfaches Nutzungsrecht an den Softwarepflegeprodukten.

8.5 Wurde die Softwarepflege nicht rechtzeitig verlängert, besteht die Möglichkeit, dass der Lizenznehmer rückwirkend die Softwarepflege erwirbt. Der 12-Monatszeitraum der neu erworbenen Softwarepflege läuft ab dem Zeitpunkt des Endes des vorhergehenden Softwarepflegezeitraums.

8.6 Softwarepflege und Support Private
Private ist nur für die Privatanwenderprodukte verfügbar und beinhaltet Updates innerhalb einer Version für die nächsten 12 Monate. Upgrades auf die nächsthöhere Version sind nicht inbegriffen. Darüber hinaus ist ein Email-Support werktags von Montag bis Freitag an support@passwordsafe.de enthalten. Die maximale Reaktionszeit beträgt regelmäßig nicht mehr als 72 Stunden, im Einzelfall kann es zu einer zeitlichen Überschreitung kommen.

8.7 Softwarepflege und Support Company Classic
Company Classic beinhaltet sowohl Updates innerhalb der nächsten 12 Monate einer Version sowie des Upgrade auf die nächsthöhere Version, soweit dies innerhalb von 12 Monaten nach dem Kauf geschieht. Darüber hinaus ist ein Email-Support werktags von Montag bis Freitag an support@passwordsafe.de enthalten. Die maximale Reaktionszeit beträgt regelmäßig nicht mehr als 48 Stunden, im Einzelfall kann es zu einer zeitlichen Überschreitung kommen.

8.8 Softwarepflege und Support Company Premium
Company Premium beinhaltet Updates und Upgrades innerhalb der nächsten 12 Monate. Zudem gehört zum Leistungsumfang kostenloser Email-Support (support@passwordsafe.de) werktags von Montag bis

Freitag, der Telefonsupport und eine Hilfe per Fernzugriff (TeamViewer). Die maximale Reaktionszeit beträgt regelmäßig nicht mehr als 24 Stunden, im Einzelfall kann es zu einer zeitlichen Überschreitung kommen.

8.9 Produktschulungen können separat erworben werden.

8.10 Der Support via Telefon, Email und Fernzugriff dient lediglich der Unterstützung/Beratung bei der Anwendung oder bei der Fehlersuche. Ein Erfolg wird dabei nicht geschuldet.

8.11 Die Pflicht des Kunden zur Bezahlung des Entgelts für die Softwarepflege besteht unabhängig von der Inanspruchnahme der Softwarepflegeprodukte.

9. Haftung

9.1 MATESO haftet nur für Schadenersatzansprüche des Kunden aus der Verletzung des Lebens, des Körpers, der Gesundheit oder aus der Verletzung wesentlicher Vertragspflichten (Kardinalspflichten) sowie die Haftung für sonstige Schäden, die auf einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung von MATESO, der gesetzlichen Vertreter oder Erfüllungsgehilfen beruhen. Wesentliche Vertragspflichten sind solche, deren Erfüllung zur Erreichung des Vertragsziels notwendig ist. Eine weitergehende Haftung ist ausgeschlossen.

9.2 Die Haftung bei Verletzung wesentlicher Vertragspflichten ist auf den vertragstypischen, vorhersehbaren Schaden beschränkt, wenn dieser einfach fahrlässig verursacht wurde, es sei denn, es handelt sich um Schadenersatzansprüche des Kunden aus einer Verletzung des Lebens, des Körpers oder der Gesundheit.

9.3 Werden Ansprüche direkt gegen gesetzliche Vertreter und Erfüllungsgehilfen von MATESO geltend gemacht, gelten die Einschränkungen der vorstehenden Abschnitte auch zu deren Gunsten.

9.4 Die Vorschriften des Produkthaftungsgesetzes bleiben unberührt.

10. Schriftformklausel

Mündliche Nebenabreden wurden nicht getroffen. Änderungen und Ergänzungen dieser Bedingungen bedürfen der Schriftform. Dies gilt auch für diese Klausel.

11. Gerichtsstand

Im Verhältnis zu Kaufleuten, juristischen Personen oder öffentlich-rechtlichen Sondervermögen ist Erfüllungsort und ausschließlicher Gerichtsstand für alle sich aus dem jeweiligen Vertragsverhältnis ergebenden Streitigkeiten Augsburg.

12. Schlussbestimmungen

12.1 Auf Verträge zwischen MATESO und den Kunden findet das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts Anwendung.

12.2 Sollten einzelne Klauseln dieser allgemeinen Geschäftsbedingungen unwirksam sein, werden die übrigen Bestimmungen davon nicht berührt. Anstelle der unwirksamen Punkte treten, soweit vorhanden, die gesetzlichen Vorschriften. Soweit dies für eine Vertragspartei eine unzumutbare Härte darstellen würde, wird der Vertrag jedoch im Ganzen unwirksam.

12.3 Vertragssprache ist Deutsch. Bei Auslegungsproblemen und sprachlich bedingten Diskrepanzen zwischen der ausländischen und der deutschen Fassung ist die deutsche Fassung maßgeblich.